YEAR 2000 COMPLIANCE EFFORT AT THE BUREAU OF ALCOHOL, TOBACCO AND FIREARMS

OIG-99-021 **DECEMBER 18, 1998**

Office of Inspector General

****

United States Department of the Treasury

December 18, 1998

MEMORANDUM FOR JOHN W. MAGAW, DIRECTOR
BUREAU OF ALCOHOL, TOBACCO AND FIREARMS

FROM: David C. Williams
Inspector General

SUBJECT: Year 2000 Compliance Audit

This memorandum transmits our final audit report titled Year 2000 Compliance Effort at the Bureau of Alcohol, Tobacco and Firearms (ATF). We are reporting our findings and nine recommendations to strengthen ATF's Year 2000 compliance effort based on our audit work performed from April through July 1998. Subsequent work performed by us will be reported to you in a separate report.

This audit disclosed that additional actions are needed in the areas of project management, system conversion and certification, data exchanges, and contingency planning for business continuity in order to mitigate the risk of a disruption in business on January 1, 2000. During the audit, we identified specific issues in these areas which should be addressed, and we promptly brought them to your managers' attention.

Our findings are summarized in the Overview and explained in further detail in the Audit Results sections of the report. Also, the nine recommendations we are making to reduce ATF's risk of a Year 2000 induced failure are contained in the applicable sub-sections of the Audit Results.

The response to findings and recommendations included in our draft report have been incorporated into the report. In addition, a complete text of ATF's response is presented in Appendix 2 at the end of the report.

We appreciate the courtesies and cooperation provided to our auditors during the audit. If you wish to discuss this report, you may contact me at (202) 927-5400 or a member of your staff may contact Barry L. Savill, Director of Audit at (202) 283-0151.

Attachment

Overview

This report presents the results of our audit to determine if the Bureau of Alcohol, Tobacco and Firearms (ATF) established an infrastructure for managing its conversion effort and minimizing the risk that a Year 2000 induced failure would have on its operations. Our specific objectives were to evaluate ATF's Year 2000 effort for the following: (1) project management; (2) system conversion and certification; and (3) contingency plans for business continuity.

Our audit found that ATF had an infrastructure, skilled resources, and reasonable guidance in place to address its Year 2000 conversion task. However, the issues presented below need to be addressed to aid ATF's conversion efforts to mitigate the risk of a Year 2000 induced failure on its operations.

- Project management should be further strengthened by: developing performance measures to ensure accountability; and taking the appropriate action to ensure continuity in contracted support.

- System conversion process and certification plans should be further strengthened by: coordinating cross-functional activities; formalizing the Year 2000 compliance testing procedures; minimizing concurrent development; and improving configuration management for maintaining conversion integrity.

- Data exchanges testing strategies should be improved by including the necessary coordination with data exchange partners.

- Contingency planning should be further strengthened by: accelerating the timeline for developing and testing contingency plans; and developing the plans on a prioritized basis.

We are making nine recommendations for corrective action. These recommendations are designed to strengthen ATF's Year 2000 conversion process, and, upon implementing the recommendations, we believe ATF's risk of any Year 2000 induced failure will be reduced.

Background

The upcoming century change is considered to be one of the most critical problems facing information technology (IT) professionals today. The Year 2000 problem results from how dates are recorded and processed in many computer systems. Systems have typically used two digits to represent the year, such as "98" for 1998, in order to conserve on electronic data storage and cost. With this two digit format, however, the Year 2000 is indistinguishable from 1900, 2001 from 1901, and so on. As a result of this ambiguity, system or application programs that use dates to perform calculations, comparisons, or sorting may generate incorrect results when working with years after 1999. The Year 2000 dilemma affects everyone, and its deadline is fixed.

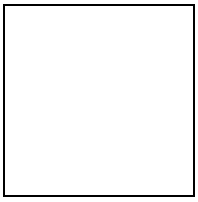
ATF is a law enforcement organization responsible to reduce crime, collect revenue, and protect the public. ATF fulfills these responsibilities by enforcing Federal laws and regulations related to alcohol, tobacco, firearms, explosives, and arson by working directly and in cooperation with others. Many of ATF's operations are reliant upon date sensitive computerized systems. Management's Year 2000 strategy for its 24 mission critical systems is to replace most of ATF's mainframe legacy systems by migrating to a client-server environment.

In ATF's June 1998 monthly status report, ATF reported 24 mission critical systems of which:

- 5 systems were implemented and certified as Year 2000 compliant;
- 13 systems were implemented and pending certification; and
- 6 replacement systems were currently being developed.

ATF's independent validation and verification process was designed to certify within a test environment a production copy of the application as Year 2000 compliant. Prior to certification, systems implemented included both systems replaced and systems that were originally assessed compliant. Chart 1 illustrates ATF's conversion progress on its 24 mission critical IT systems.

Chart 1



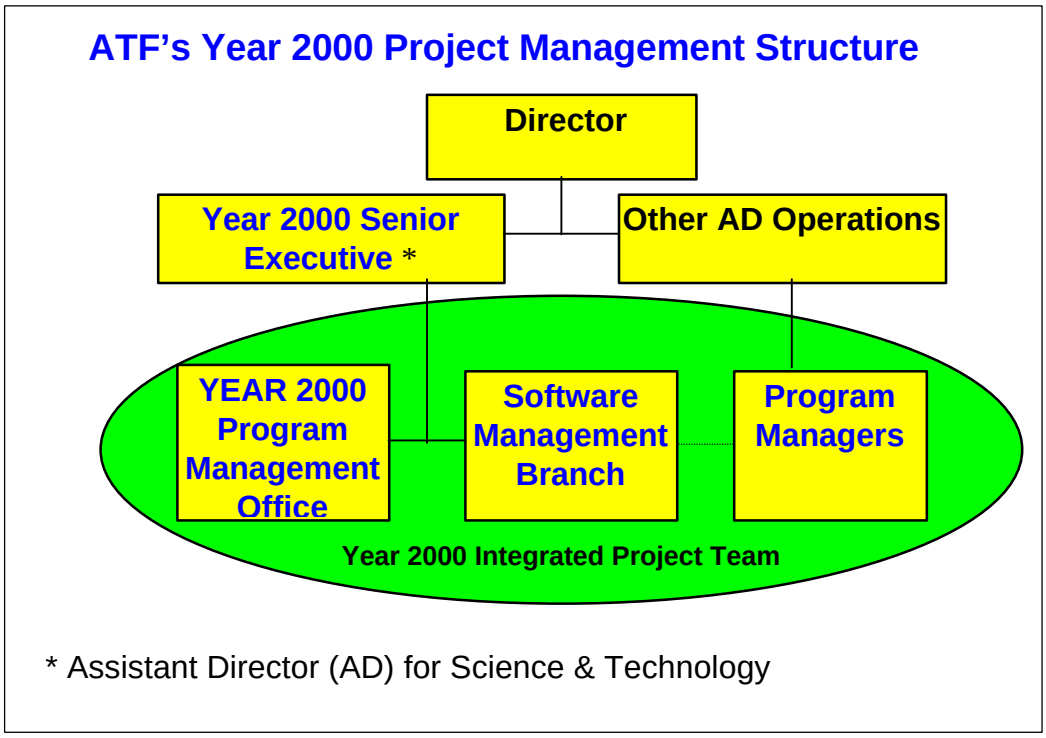
Source: ATF's June 1998 monthly status report

To address ATF's Year 2000 issues, the Assistant Director, Office of Science and Technology / Chief Information Officer was designated as the Year 2000 Senior Executive. Under the Year 2000 Senior Executive, the Year 2000 Program Management Office (PMO) was established to:

- increase awareness throughout ATF;
- oversee the bureau's Year 2000 efforts;
- track and report project status to the Department of the Treasury's Year 2000 Project Office (Department); and
- perform system certification.

The Software Management Branch (SMB) was responsible for making ATF's systems Year 2000 compliant. The Program Managers (PM) represent officials from other areas of ATF's organization that were assigned to the Year 2000 project as user representatives from their functional areas. Together, the PMO, SMB, and the PMs made up ATF's Year 2000 Integrated Project Team (IPT) tasked to implement ATF's Year 2000 compliance effort as depicted in chart 2.

Chart 2



Source: OIG

Objectives, Scope and Methodology

The overall objective of our audit was to evaluate ATF's Year 2000 conversion effort on its mission critical IT systems. In addition, we performed a limited review of ATF's strategy and progress on its non-IT and telecommunication systems. Our audit was designed to determine if ATF management established an infrastructure for managing its conversion effort and minimizing the risk that a Year 2000 induced failure would have on its operations. Our specific objectives were to evaluate ATF's Year 2000 effort for the following: (1) project management; (2) system conversion and certification; and
(3) contingency plans for business continuity.

To accomplish our objectives, we performed field work from April through July 1998. We reviewed applicable Year 2000 documentation, including: Treasury's Year 2000 Vulnerability Assessment Report dated October 1997; ATF's monthly status reports; ATF's Year 2000 Project Plan, and other related documents. In addition, we interviewed the appropriate officials within the Office of Science and

Technology and ATF's contractor who had responsibilities for the Year 2000 effort.

Our review was solely limited to evaluating strengths and weaknesses in the management of the Year 2000 conversion project. Specifically, we determined if processes existed, appeared reasonable, and were designed to mitigate the Year 2000 risk to an acceptable level for ensuring all mission critical IT systems remain operable. This report is not intended to represent or convey statements that any given system is Year 2000 compliant or that a system will or will not work into the next millennium.

A list of abbreviations used in this report is attached as Appendix 1.

This audit was conducted in accordance with Government Auditing Standards issued by the Comptroller General of the United States, and included such audit tests as were deemed necessary.

Audit Results

Project Management

ATF had taken positive steps towards managing its Year 2000 compliance effort. In addition to the accomplishments discussed later in this report, ATF assigned competent and knowledgeable personnel to perform ATF's Year 2000 conversion effort. However, project management could be further strengthened to reduce the Year 2000 risk impact by: (1) developing performance measures to ensure accountability; and (2) taking the appropriate action to ensure continuity in contracted support. Failure to strengthen the project management in these areas could increase the project risk associated with managing this Year 2000 effort.

Guidance provided in the Department's Project Management Plan, section 2.3.2, "Bureau / Office Roles and Responsibilities," stated that each bureau Year 2000 project management infrastructure is responsible for the planning, execution, and reporting of their conversion progress. In addition, section 10.1, "The Risk Management Process," holds program officials responsible for assessing, monitoring and controlling risks associated with Year 2000 conversion projects.

Individual Year 2000 Performance Measures

While ATF established the IPT to manage the Year 2000 project, all of its executive managers were ultimately responsible to ensure Year 2000 issues were resolved in a timely and effective manner. However, not all of ATF's personnel with Year 2000 conversion responsibility, such as the business users[1] who were responsible to prepare business contingency plans, had formal performance measures. Without formal accountability measures, executives along with their supporting staff may defer responsibility to the Year 2000 Senior Executive and the IPT. Also, they may not fully recognize their responsibility for ensuring that ATF systems are compliant and that contingencies for business continuity exist.

Year 2000 Contractor Support

ATF substantially relied on contracted resources for its Year 2000 conversion. However, during our field work, the contract was potentially in jeopardy due to concerns raised by the Small Business Administration (SBA) about issuing a sole-source contract. This specific contractor had been on board since the initial assessment work. As such, the contractor and the contractor's staff possessed the knowledge of and familiarity with ATF and the Year 2000 issues. Therefore, ATF believed extending the contract was justified.

During the time of our review, ATF management and Department officials were actively addressing SBA's concerns. Given the time constraints posed by the unyielding date of January 1, 2000, the money and effort required to obtain and familiarize another contractor would introduce a significant risk to the Year 2000 project.

Recommendations

1. The ATF Director should ensure that performance measures or other means of assigning accountability are developed and implemented for all of ATF's personnel with responsibility for the Year 2000 compliance effort, such as executive managers and system and business users.

   Management Response and OIG Comment

   ATF concurred with this recommendation and stated that ATF is confident its individual performance appraisal processes provide required accountability needed for personnel involved in all aspects of

[1] Business users are groups or individuals who receive, use, or are directly affected by the IT system's operation.

the Year 2000 effort. As one of the top priorities of the Director, managers are using current performance critical elements to assign and measure Year 2000 related tasks to employees. ATF's performance measurement process incorporates all critical activities that are relevant to the strategic mission goals and measures the attainment of the respective goals. The Strategic Planning Office is overseeing ATF's performance measurement process and its ability to measure Year 2000 goals against resources and performance.

The OIG concurs with ATF's actions.

2. Absent any contractual violations, the ATF Director should ensure that appropriate action is taken to preserve the contracting vehicle for its Year 2000 conversion in order to maintain the project team continuity.

Management Response and OIG Comment

ATF concurred with this recommendation and stated that ATF has addressed and resolved this issue through the use of the General Services Administration Schedule to retain Year 2000 contractor continuity. ATF has worked with the contractor to find various ways to retain the Year 2000 expertise and knowledge of its system, including formally recognizing the value and contributions of the contractors.

The OIG concurs with ATF's actions.

System Conversion and Certification

ATF's Year 2000 conversion process and certification plans appeared to be comprehensive and set forth clear certification criteria. SMB was assigned the responsibility to perform system renovation and replacement, functional testing, and implementation. Upon implementation, PMO was assigned the responsibility to certify the application within the certification test environment.

While the above was a positive effort, the processes could be further strengthened to reduce the Year 2000 risk impact by: (1) coordinating cross-functional activities; (2) formalizing the Year 2000 compliance testing procedures; (3) minimizing concurrent development; and

(4) improving configuration management for maintaining conversion integrity.

Guidance provided in the Treasury Year 2000 Date Conversion Program Management Plan, section 2.3.2, "Bureau / Office Roles and Responsibilities," stated that each bureau Year 2000 project management infrastructure is responsible for the planning, execution, and reporting of their conversion progress. In addition, section 10.1, "The Risk Management Process," holds program officials responsible for assessing, monitoring and controlling risks associated with Year 2000 conversion projects.

Cross-Functional Coordination

Conversion schedule variances existed between PMO and SMB because a mechanism was not established to coordinate their Year 2000 effort. Coordination was needed due to PMO's dependence on SMB's responsiveness, scheduling decisions, and on-going communication about changes. Specifically, certification testing could not be planned until SMB implementation dates were known, and the testing could not be performed until applications were actually implemented. In the meantime, however, SMB's workload was driven by an ambitious schedule to migrate ATF's systems to a client-server environment.

Based on our review, the examples below demonstrate conversion schedule variances we identified.

- PMO was focused on mission critical systems, and SMB's workload over the next year included both mission critical and non-mission critical projects. However, PMO was subject to Departmental and Office of Management and Budget (OMB) milestone dates through March 1999, whereas the SMB implementation dates for mission critical systems extend beyond that milestone date.

- Both offices maintained separate schedules with differences in system implementation dates, number of systems in total, and number of mission critical systems.

- Several systems assessed as compliant and ready for certification by PMO were actually scheduled for replacement by SMB.

- SMB made frequent changes to their schedule. These continuous changes rendered the information obtained and reported by PMO to the Department as inaccurate, and PMO's workload estimates inconsistent.

During our field work, we brought the above issues to the attention of the ATF staff assigned to the compliance effort. Consequently, PMO and SMB staff members held on-going meetings to reconcile the schedules. Additionally, the Year 2000 Senior Executive advised us that a process will be put in place to coordinate the effort of the two offices, and an individual will be assigned to monitor the schedules to ensure they remain in synch.

Formalize Year 2000 Compliance Testing

No evidence existed that ATF was requiring all functional testing to include Year 2000 testing criteria for all applications prior to implementation. Also, the Year 2000 compliance criteria and test plans were developed by the contractor without formal adoption by ATF personnel. Failure to formally incorporate Year 2000 testing would result in placing the sole burden on the certification process to identify instances of non-compliance.

By design, the certification testing occurs after implementation. Accordingly, by the time an instance of non-compliance is identified, adequate lead time may not be available to send the application back through development, re-implementation, and re-certification. Given that ATF was delayed in implementing its certification process, the certification testing schedule was already ambitious.

Minimize Concurrent Development

A policy was not developed to minimize non-essential system development, including enhancements and modifications. As previously discussed, SMB's migration schedule was ambitious. Their workload over the next year included migrating both mission critical and non-mission critical systems to a client-server environment and accommodating all system development requests. If SMB's workload is not properly prioritized, ATF's ability to meet its Year 2000 compliance objectives may be jeopardized.

Improve Configuration Management

ATF had not taken action on their contractor's recommendation to strengthen the configuration management practices. The process did not ensure that the:

- correct version of an application was staged for production;
- same version implemented was sent to certification testing; and
- subsequent modifications and environmental changes did not nullify the Year 2000 certified versions.

Failure to adopt an adequate configuration management process could undermine the integrity of the certification test results and nullify assurance from certified systems.

3. The ATF Director should ensure that overall responsibility and sufficient authority are assigned to direct and oversee the cross-functional Year 2000 compliance effort. This oversight should include the prompt evaluation of the PMO and SMB schedules to make the necessary modifications to ensure that objectives, priorities, and timelines are coordinated to best position ATF to meet its Year 2000 compliance objective.

   Management Response and OIG Comment

   ATF concurred with our recommendation and stated that the Chief, Information Services Division (ISD), is actively overseeing the Year 2000 cross-functional activities and compliance efforts. The Chief's direct involvement includes a weekly progress review and issue meeting and the preparation of a joint Year 2000 compliance testing, migration, and certification schedule. ATF also stated that, at the functional level, the Year 2000 PMO, SMB, and the Operations Support Branch meet biweekly to address individual and joint issues that impact Year 2000 milestones.

   The OIG concurs with the actions taken by ATF.

4. The ATF Director should require Year 2000 compliance testing prior to implementing applications, and designate an ATF official to review and approve the test results.

   Management Response and OIG Comment

ATF concurred with this recommendation and stated that ATF has adopted Year 2000 compliance testing criteria and is in the process of documenting the use of this testing criteria in its software development process. ATF expects to complete this documentation by December 1, 1998. In addition, the Year 2000 Senior Executive has designated the Chief, ISD, as the reviewing and approving official for all Year 2000 compliance testing.

The OIG concurs with the actions taken by ATF.

5. The ATF Director should establish a policy to restrict concurrent development, specifically enhancements and modifications, through the critical Year 2000 conversion period. This restriction should allow for and include provisions and criteria for emergency related changes.

Management Response and OIG Comment

ATF did not concur with this recommendation. ATF stated that it feels its current software development program oversight practices achieve the same objective. ATF stated that its IT policymaking body is the Information Resources Management (IRM) Council and that one of the Council's responsibilities is to prioritize all applications development, enhancements, and modifications in support of ATF business processes. IRM Council decisions are heavily influenced by external factors, such as statutory and regulatory requirements. However, as the chair of the IRM Council, the Year 2000 Senior Executive ensures Year 2000 issues are considered in all IT system decisions.

ATF's Year 2000 Senior Executive has mandated that development of replacement applications be restricted to mission critical systems. However, enhancements and modifications to non-mission critical systems are also controlled by the IRM Council and influenced by external factors. Upon IRM Council decisions, the system sponsor controls application requirements to prevent non-approved system changes that could delay production, implementation and Year 2000 certification.

Although ATF did not concur with this recommendation, we believe ATF's actions satisfy the intent of the recommendation.

6. The ATF Director should require that sound configuration management practices are identified and applied to ensure consistency in new

application implementations, as well as to ensure that the integrity of certification results are preserved.

Management Response and OIG Comment

ATF concurred with this recommendation. ATF stated that configuration management practices were identified, and ATF anticipates a formalized process to be implemented no later than February 1999. The Chief, ISD, has been tasked to oversee the configuration management effort through the Chief Financial Officer's Electronic Data Processing Team.

The OIG concurs with ATF's actions.

Data Exchanges With Trading Partners

ATF identified its data exchange partners, but had no plans to coordinate testing of these interfaces with their trading partners. Electronic data exchanges are used extensively to transfer information between computer systems and other entities. Consequently, as computer systems are converted to process Year 2000 dates, the associated data exchanges must also be made Year 2000 compliant. If Year 2000 data exchange problems are not corrected, the adverse impact could be severe. If these exchanges do not function properly, data will either not be exchanged between systems, or produce invalid data which could cause receiving computer systems to malfunction or produce inaccurate computations.

In OMB Memorandum 98-02, agencies were directed to inventory all data exchanges with outside partners and to determine a transition plan. A transition plan is the strategy for dealing with data exchange that at a minimum includes agreed upon date format, conversion responsibilities, time frames, and testing arrangements.

ATF planned to unilaterally test the interfaces as part of their system testing. This testing may be adequate for modifications made to interfaces they are responsible for maintaining, but the strategy excludes those interfaces maintained by their partners. By not coordinating testing efforts with their data exchange partners, ATF has no assurance that the exchange of data will continue without disruption beyond the system encounter date.[2]

[2] Encounter date is the known date that the system will fail, or be negatively impacted. This date could be on or before January 1, 2000.

7. To strengthen data exchange practices, the ATF Director should require the conversion effort to include the necessary coordination with data exchange partners during the testing phase.

Management Response and OIG Comment

ATF concurred with our recommendation and stated that the Year 2000 Senior Executive has assigned Data Exchange oversight of the SMB data exchange efforts to the Year 2000 PMO. The Year 2000 PMO will assess data exchange compliance through proactive involvement with data exchange partners, ATF users, and SMB concurrently with their testing efforts. The Year 2000 PMO will ensure data exchange testing procedures are incorporated into the compliance testing process. ATF expects formal documentation of these procedures by January 30, 1999.

The OIG concurs with ATF's actions.

Contingency Plans for Business Continuity

ATF's Year 2000 contingency planning guidance appropriately included the business users as being responsible for developing business contingency plans in the event business operations are impacted by a Year 2000 system failure. However, the timeline for developing and testing these plans needs to be accelerated. In addition, the contingency plans should be developed on a prioritized basis. Prioritization factors should include the current renovation progress measured against established milestones, system encounter dates and system criticality.

During our field work, ATF's emphasis was on conversion. However, as the encounter dates rapidly approach, ATF should recognize the critical need for developing and implementing sound and reliable business continuity plans. If the required plans are not timely developed, tested, and formalized, ATF may not be able to ensure the continuity of its core business processes in the event of Year 2000 induced failure.

The Treasury Year 2000 Date Conversion Program Management Plan directed bureaus to ensure the continuity of essential operations. Each bureau was to develop contingency plans that addressed the failure of systems believed to be Year 2000 compliant, and operational alternatives for systems that will not be Year 2000 compliant by the needed date, as appropriate. Contingency plans were due to the Department by September

1998. OMB Circular 98-02 requires contingency plans for mission critical systems: not implemented before March 1999; and 2 or more months behind schedule.

Contingency plans for business continuity should address risks not only with internal systems, but external risks with business partners and the public infrastructure. The plan should identify resources, procedures, and appropriate training required to carry out core business functions. Plans should be tested thoroughly and continuously re-evaluated. Steps should be included that facilitate the restoration of normal services at the earliest possible time.

Based on our review of ATF's contingency planning guidance and draft plans, we identified the issues listed below which require management's attention.

- ATF had not developed a schedule that identifies, prioritizes, and lays out the timeline for the development and testing of contingency plans for each mission critical system. Consequently, ATF may not be able to develop and test contingency plans by the established milestone date.

- ATF had not identified encounter dates for each of their mission critical systems during the assessment stage. Because some information systems use future dates, it is likely that these systems will fail before January 1, 2000. Therefore, the risk exists that ATF may encounter an unanticipated failure which could severely affect operations but contingency plans may not yet be in place.

- ATF planned to test contingency plans for non-IT systems through December 31,1999. However, if contingency plans are not tested until late 1999, there may not be time to develop alternative plans. Critical dependencies on non-IT systems could cause a major disruption to their business operations.

- Aside from ATF's outreach initiative for its revenue operations, ATF's had not developed business continuity plans for its other business operations.

8. The ATF Director should accelerate and prioritize the due dates for developing and testing contingency plans for IT and non-IT mission critical systems based on: systems with early encounter dates; systems

that are 2 or more months behind schedule; systems with implementation dates after March 1999; and other mission critical systems.

Management Response and OIG Comment

ATF concurred with our recommendation and stated that it has completed continuity of operations plans for all IT and non-IT mission critical systems. ATF expects testing will be accomplished throughout the Calendar Year 1999 and updates will be applied as needed.

The OIG concurs with ATF's actions.

9. The ATF Director should direct the development of a business continuity plan to ensure all core business processes will continue to function at an acceptable level in the event of a Year 2000 induced failure.

Management Response and OIG Comment

ATF concurred with our recommendation and stated that the Director will be discussing the development of a Bureau-level business continuity plan with the Executive Staff and assigning responsibility.

The OIG concurs with ATF's actions.

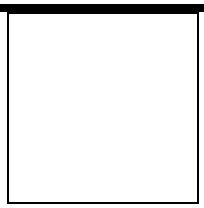
Conclusion

Our review was solely limited to evaluating strengths and weaknesses in the management of the Year 2000 conversion project. Specifically, we determined if processes existed, appeared reasonable, and were designed to mitigate the Year 2000 risk to an acceptable level for ensuring all mission critical IT systems remain operable. In addition, we performed a limited review of ATF's strategy and progress on its non-IT and telecommunications systems. We determined in the event of a Year 2000 induced failure that alternative resources and processes needed to operate ATF's core business processes had been identified. As such, this report is not intended to represent or convey statements that any given system is Year 2000 compliant or that a system will or will not work into the next millennium. While we recognize that Year 2000 remediation is the responsibility of ATF's management and system owners, we are making nine recommendations for corrective action. These recommendations are designed to strengthen ATF's Year 2000 conversion process, and, upon implementing the recommendations, we believe ATF's risk of any Year 2000 induced failure will be reduced.

ABBREVIATIONS

AD	Assistant Director
ATF	Bureau of Alcohol, Tobacco and Firearms
Department	Department of the Treasury's Year 2000 Project Office
IPT	Integrated Project Team
IRM	Information Resources Management
ISD	Information Services Division
IT	Information Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PM	Program Manager
PMO	Program Management Office
SBA	Small Business Administration
SMB	Software Management Branch

MANAGEMENT RESPONSE



MANAGEMENT RESPONSE

ATF Response
to the
Year 2000 Compliance Audit
Bureau of Alcohol, Tobacco & Firearms

November 1, 1998

Introduction

This document responds to the results of the Department of Treasury Office of Inspector General (OIG) audit conducted July 1998. It should be noted OIG conducted a fair and professional examination of the Bureau's Year 2000 (Y2K) effort.

The Bureau of Alcohol, Tobacco and Firearms (ATF) Y2K Compliance strategy incorporates two major executive business decisions: the Bureau's mainframe-to-client-server migration strategy and standardization of developmental commercial-off-the-shelf (COTS) software as part of our Enterprise Systems Architecture (ESA) initiative. The intent of this strategy is to move the Bureau technically into the 21st century, provide ATF personnel better systems to assist them in meeting ATF strategic goals and to minimize risks of any Y2K impacts.

Operationally, all ATF Directorates are involved in Y2K preparations. However, ATF's focal point for all activities within and out of the Bureau is the Y2K Senior Executive. He ensures all Y2K issues are addressed in the attainment of all ATF mission goals and Y2K accountability are realized.

The following audit response reflects the progress ATF has accomplished to date, and provides requested replies to your audit findings and recommendations.

MANAGEMENT RESPONSE

Audit Result Responses

Project Management

1. **Finding**

Lack of formal accountability measures for ATF personnel allows for executives and supporting staff to defer responsibility to the Year 2000 Executive and supporting Integrated Project Team (IPT).

Recommendation

ATF Director should ensure that performance measures or other means of assigning accountability are developed and implemented for all of ATF's personnel with responsibility for the Y2K compliance effort, such as executive managers and system and business users.

ATF response

Respectfully concur with finding and recommendation.

ATF is confident its individual performance appraisal processes provide required accountability needed for personnel involved in all aspects of the Y2K effort. As one of the top priorities of the Director, managers are using current performance critical elements to assign and measure Y2K related tasks to employees. The success ATF just recently had in drafting contingency plans for its mission-critical IT and Non-IT systems is an example of Y2K performance accountability.

Strategically, the Bureau's performance measurement process incorporates all critical activities that are relevant to the strategic mission goals and measures the attainment of the respective goals. Year 2000 is one of those activities. The Strategic Planning Office is overseeing the Bureau's performance measurement process and its ability to measure Y2K goals against resources and performance.

2. **Finding**

Significant Y2K project risk would be introduced if Y2K contractor continuity was jeopardized due to contract extension issues.

Recommendation

Absent any contractual violations, the ATF Director should ensure the appropriate action is taken to preserve the contracting vehicle for its Year 2000 conversion in order to maintain the project team continuity.

MANAGEMENT RESPONSE

ATF Response

Respectfully concur with finding and recommendation.

ATF has addressed and resolved this issue through the use of the General Services Administration (GSA) Schedule to retain Y2K contractor continuity. Additionally, ATF has worked with the contractor to find various ways to retain the Y2K expertise and knowledge of our systems. For example, the Y2K Program Management Office (PMO) is formally recognizing the value and contributions of our Y2K contractors and is continuously recognizing their contributions by providing letters of "Special Achievement" to their management staff. Concurrently, the contractor supporting the Bureau's Y2K effort intends to use project completion bonuses to retain required skills.

System Conversion and Certification

3. Finding

ATF lacked process to coordinate the efforts of the Y2K PMO and the Software Management Branch (SMB) and did not have an individual assigned to monitor the conversion, migration and certification schedules to ensure they remain in sync.

Recommendation

The ATF Director should ensure that the overall responsibility and sufficient authority is assigned to direct and oversee the cross-functional Y2K compliance effort. This oversight should include the prompt evaluation of PMO and SMB schedules to make the necessary modifications to ensure that the objectives, priorities, and timelines are coordinated to best position ATF to meet its Y2K compliance objective.

ATF Response

Respectfully concur with finding and recommendation.

Y2K success requires an integrated and collaborative effort between the Y2K PMO and SMB. This has been accomplished with the Chief, Information Services Division (ISD) actively overseeing the Y2K cross-functional activities and compliance efforts. Specifically, his direct involvement includes a weekly progress review and issue meeting and the preparation of a joint Y2K compliance testing, migration and certification schedule. At the functional level, the Y2K PMO, SMB and the Operations Support Branch meet biweekly to address individual and joint issues that impact Y2K milestones. These actions have provided

MANAGEMENT RESPONSE

an effective forum to address and resolve all conversion, migration and certification schedules.

Additionally, the Y2K Senior Executive is briefed twice monthly, once with the Y2K PMO regarding Y2K status concurrent with the Treasury monthly reporting cycle and again to address Y2K cross-functional efforts via our Integrated Project Team (IPT) meetings.

4. Finding

No evidence existed that ATF was requiring all functional testing to include Y2K testing criteria for all applications prior to implementation. Also, Y2K Compliance testing criteria and processes had not been formally adopted by ATF personnel.

Recommendation

The ATF Director should require Y2K compliance testing prior to implementing applications, and designate an ATF official to review and approve test results.

ATF Response

Respectfully concur with finding and recommendation.

While Y2K compliance testing is being performed prior to production implementation this procedure has yet to be documented. ATF has adopted Y2K compliance testing criteria. We are in the process of documenting the use of our Y2K compliance testing criteria in our software development process. We anticipate completing this documentation by December 31, 1998. In addition, the Y2K Senior Executive has designated the Chief, ISD as the reviewing and approving official for all Y2K compliance testing.

5. Finding

ATF does not have a policy in place to minimize non-essential system development, including enhancements and modifications. If SMB's workload is not properly prioritized, ATF Y2K objectives could be jeopardized.

Recommendation

The ATF Director should establish a policy to restrict concurrent development, specifically enhancements and modifications, through the critical Y2K conversion period. This restriction should allow for and include provisions and criteria for emergency related changes.

MANAGEMENT RESPONSE

ATF Response

Respectfully non-concur with the finding and recommendation.

While it is true a policy does not exist to restrict concurrent development, we feel our current software development program oversight practices achieve the same objective.

ATF's Information Technology (IT) policymaking body is the Information Resources Management (IRM) Council. One of the Council's responsibilities is to prioritize all applications development, enhancements and modifications in support of ATF business processes. ATF's business strategy is to assess old systems that support the Bureau's mission, determine their viability, Y2K compliance, and the necessary replace or repair actions. Many existing mission critical systems have been assessed for Y2K compliance and those that required renovation in all cases were deemed to be best addressed as part of their Bureau migration strategy. Also, IRM Council decisions are heavily influenced by external factors, such as statutory and regulatory requirements. As the chair of the IRM Council, the Y2K Senior Executive ensures Y2K issues are considered in all IT system decisions.

Our Y2K Senior Executive has mandated that development of replacement applications be restricted to mission critical systems. However, enhancements and modifications to non-mission critical systems are also controlled by the IRM council and influenced by the same factors as stated above.

Upon IRM Council decisions, the system sponsor controls application requirements to prevent non-approved system changes that could delay production, implementation and Y2K certification.

6. Finding

ATF failure to adopt an adequate configuration management process could undermine the integrity of the certification test results and nullify assurance for certified systems.

Recommendation

The ATF Director should require that sound configuration management practices are identified and applied to ensure consistency in new application implementations, as well as to ensure that the integrity of certification results are preserved.

MANAGEMENT RESPONSE

ATF Response

Respectfully concur with finding and recommendation.

This finding was also identified during the recent Chief Financial Officer's (CFO) Audit. As a result, configuration management practices were identified, and are being applied to a formalized process. We anticipate a formalized process to be implemented no later than February 1999. The Chief, ISD has been tasked to oversee the configuration management effort through the CFO Electronic Data Process Team. The Team was established to correct all CFO Audit findings, including configuration management.

Data Exchange with Trading Partners

7. Finding

ATF has no plans to coordinate testing of interfaces with trading partners. ATF has no assurance that the exchange of data will continue without disruption beyond the system encounter date with unilateral testing.

Recommendation

To strengthen data exchange practices, the ATF Director should require the conversion effort to include necessary coordination with data exchange partners during the testing phase.

ATF Response

Respectfully concur with finding and recommendation.

The ATF Y2K Senior Executive has assigned Data Exchange oversight of the SMB data exchange efforts to the Y2K PMO. The Y2K PMO will assess data exchange compliance through pro-active involvement with data exchange partners, ATF users and SMB concurrent with their compliance testing efforts. The Y2K PMO will ensure data exchange-testing procedures are incorporated into the compliance testing process. We anticipate formal documentation of these procedures by January 30, 1999.

MANAGEMENT RESPONSE

Contingency Plans for Business Continuity

8. Finding

ATF has not developed a schedule that identifies, prioritizes and lays out the timeline for the development and testing of contingency plans for each mission critical system. ATF has not identified encounter dates that trigger the need of a contingency plan prior to January 1, 2000. ATF plans to test Non-Information Technology (Non-IT) contingency plans through December 31, 1999 may not leave time to develop alternative plans.

Recommendation

The ATF Director should accelerate and prioritize the due dates for developing and testing IT and non-IT mission critical contingency plans based on: systems with early encounter dates; systems that are more than two months behind schedule; systems with implementation dates after March 1999 and other mission critical systems.

ATF Response

Respectfully concur with finding and recommendation.

We have completed Continuity of Operations Plans (COOP) for all IT and non-IT mission critical systems. Development of these plans was the focus during a three day ATF Contingency Planning Conference conducted during August 1998. This conference was designed to actively engage all system owners in developing contingency plans. Plans were grouped by core business areas and addressed the continuity of the business function. These plans are currently being validated by the Y2K PMO based on the approved Bureau Contingency Planning Guide. We anticipate testing will be accomplished throughout Calendar Year (CY) 1999 and updates will be applied as needed.

9. Finding

ATF has not developed business continuity plans for its business operations.

Recommendation

The ATF Director should direct the development of a business continuity plan to ensure all core business processes will continue to function at an acceptable level in the event of Year 2000 induced failure.

MANAGEMENT RESPONSE

ATF Response

Respectfully concur with finding and recommendation.

The Director will be discussing the development of a Bureau-level business-continuity plan with the Executive Staff and assigning responsibility.

MAJOR CONTRIBUTORS TO THIS REPORT

Audit Directorate

Barry Savill, Director

Jean Purcell, Audit Manager

Don Farineau, Audit Manager

Jeanne Edwards, Team Leader

Tammy Rapp, Team Leader

Lynn Richardson, Auditor

Joseph Hardy, Auditor

REPORT DISTRIBUTION

Treasury Departmental Offices

Assistant Secretary for Management and Chief Financial Officer
Deputy Assistant Secretary for Information Systems
and Chief Information Officer
Assistant Director of Information Technology Policy and Management
Director, Office of Organizational Improvement
Director, Office of Strategic Planning
Director, Financial Management
Office of Budget
Office of Accounting and Internal Control
Management and Controls Branch

Bureau of Alcohol, Tobacco and Firearms

Director
Assistant Director, Office of Science Technology
Year 2000 Program Manager, Information Systems Management Division
Assistant Director, Office of Inspection

Office of Management and Budget

Michael S. Crowley, Budget Examiner